

(19)



Bureau voor de
Industriële Eigendom
Nederland

(11) 1011800

(12) C OCTROOI²⁰

(21) Aanvraag om octrooi: 1011800

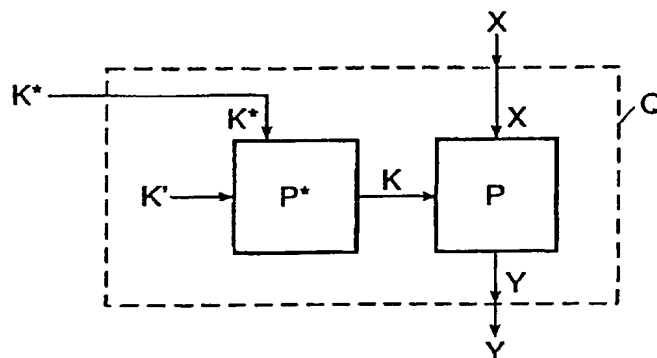
(51) Int.Cl.⁷
H04L9/06, H04L9/14, G07F7/10

(22) Ingediend: 15.04.1999

(30) Voorrang:
30.12.1998 NL 1010921
12.03.1999 NL 1011544(41) Ingeschreven:
03.06.1999 I.E. 1999/08(47) Dagtekening:
24.11.1999(45) Uitgegeven:
01.02.2000 I.E. 2000/02(73) Octrooihouder(s):
Koninklijke KPN N.V. te Groningen.(72) Uitvinder(s):
Gerrit Roelofsen te Gouda
Dirk Jan Jacobus van Bruchem te Wateringen
Frank Muller te Delft
Willem Rombout te Den Haag(74) Gemachtigde:
Drs. B. Klein te 2509 CH Den Haag.

(54) Werkwijze en Inrichting voor het cryptografisch bewerken van data.

(57) Bij het cryptografisch bewerken van data worden deze data (X) en een sleutel (K) aan een cryptografisch proces (P) toegevoerd, dat een bekend proces kan zijn. Teneinde de aard van het proces (P) te versluieren worden aan het proces hulpwaarden toegevoerd, zoals een aanvullende sleutel (K*), met behulp waarvan een aanvullend proces (P*) de eigenlijke sleutel (K) genereert. De combinatie van het oorspronkelijke proces (P) en het aanvullende proces (P*) levert een onbekend proces op, waarbij de relatie tussen de aanvullende sleutel (K*) en de bewerkte data (Y) onbekend is. Hierdoor wordt een betere cryptografische beveiliging verkregen.



AJ

NL C 1011800

De inhoud van dit octrooi komt overeen met de oorspronkelijk ingediende beschrijving met conclusie(s) en eventuele tekeningen.

toegevoerd. In dit verband wordt onder een "hulpwaarde" een waarde (data of sleutel) verstaan, die in aanvulling op de corresponderende data en sleutel aan het proces wordt toegevoerd.

5 De uitvinding is derhalve gebaseerd op het inzicht, dat het herleiden van de in een cryptografisch proces gebruikte waarden aanzienlijk gecompliceerd wordt indien deze waarden door middel van hulpwaarden zijn gemaskeerd.

De uitvinding is mede gebaseerd op het verdere inzicht, dat het gebruik van hulpwaarden het resultaat van het proces niet
10 noodzakelijkerwijs beïnvloedt.

In een eerste uitvoeringsvorm van de uitvinding omvat een hulpwaarde een aanvullende sleutel die aan een aanvullend proces wordt toegevoerd teneinde de sleutel te vormen.

Door een combinatie van een bekend proces en een aanvullend
15 proces toe te passen wordt een nieuw, op zich onbekend cryptografisch proces gevormd, zelfs indien het aanvullende proces ook op zich bekend is.

Door de voor het bekende proces gebruikte sleutel (primaire sleutel) af te leiden uit een aanvullende sleutel (secundaire sleutel)
20 met behulp van een aanvullend proces wordt bereikt dat niet de (primaire) sleutel van het bekende proces maar de aanvullende (secundaire) sleutel aan de combinatie van processen wordt aangeboden. Met andere woorden, extern wordt de aanvullende (secundaire) sleutel en niet de werkelijke (primaire) sleutel van het eigenlijke proces
25 gebruikt. Het afleiden van de sleutel uit de oorspronkelijke data en de bewerkte data is daarmee ondoenlijk geworden. Tevens is het afleiden van de aanvullende sleutel ernstig bemoeilijkt, omdat de combinatie van het oorspronkelijke proces en het aanvullende proces niet bekend is.

30 Deze uitvoeringsvorm van de uitvinding is derhalve onder meer gebaseerd op het inzicht, dat het bekend zijn van een cryptografisch proces ongewenst is, dit in tegenstelling tot wat tot dusver werd aangenomen. Deze uitvoeringsvorm is tevens gebaseerd op het verdere inzicht, dat aanvallen die voortbouwen op kennis van het proces aan-
35 zienlijk moeilijker worden indien het proces onbekend is.

Bij voorkeur omvat het aanvullende proces een cryptografisch proces. Dit maakt het herleiden van de aanvullende sleutel moeilijker. In principe kan echter bijvoorbeeld een eenvoudige codering als

1011800

worden, bij voorkeur onmiddellijk na de laatste trap, de rechter data met een verdere primaire hulpwaarde en de gemodificeerde linker data met een verdere additionele hulpwaarde gecombineerd.

Om het resultaat van de bewerkingen niet door de primaire
5 hulpwaarden te laten beïnvloeden wordt de werkwijze volgens de uitvinding bij voorkeur zodanig uitgevoerd, dat de rechter data, in elke trap en voorafgaand aan de bewerking, met de primaire hulpwaarde van die trap worden gecombineerd.

Een verdere bescherming wordt bereikt indien de bewerkte rechter
10 data, volgend op de bewerking, met een secundaire hulpwaarde van die trap worden gecombineerd.

Met voordeel is de secundaire hulpwaarde van een trap gevormd uit de combinatie van de primaire hulpwaarde van de voorgaande trap en
15 de primaire hulpwaarde van de volgende trap. Hierdoor wordt het mogelijk de hulpwaarde in de telkens volgende trap te compenseren, waardoor deze hulpwaarde niet in het eindresultaat van het proces zal doorwerken.

Het is mogelijk de werkwijze volgens de uitvinding zodanig uit
20 te voeren, dat alle primaire hulpwaarden gelijk zijn. Hierdoor is een zeer eenvoudige praktische realisatie mogelijk. Het gebruik van verschillende hulpwaarden, die bij voorkeur toevalsgetallen zijn en voor elke keer dat het proces wordt uitgevoerd opnieuw worden gegenereerd, biedt echter een grotere cryptografische beveiliging.

Een verdere vereenvoudiging van deze uitvoeringsvorm kan worden
25 verkregen indien de primaire hulpwaarden en/of secundaire hulpwaarden telkens vooraf met de respectieve bewerking zijn gecombineerd. Dat wil zeggen, het combineren met hulpwaarden wordt in de betreffende bewerking (bijvoorbeeld een substitutie) verwerkt, zodat het resultaat
30 van de respectieve bewerking gelijk is aan dat van de oorspronkelijke bewerking plus een of twee combinatiebewerkingen met hulpwaarden. Door het vooraf in de bewerking opnemen van de combinatiebewerkingen is een eenvoudiger en snellere praktische realisatie mogelijk.

De genoemde combinatiebewerkingen worden bij voorkeur door
35 middel van een exclusief-of-bewerking uitgevoerd. Andere combinatiebewerkingen, zoals binair optellen, zijn in principe echter ook mogelijk.

De uitvinding verschaft verder een schakeling voor het uitvoeren

1011800

sleutel met een voldoende grote lengte (d.w.z., een voldoende groot aantal bits) werd het tot nu toe ondoenlijk geacht deze sleutel te herleiden, zelfs indien het proces P bekend was. Ondoenlijk wil in dit geval zeggen dat het in theorie weliswaar mogelijk is, bijvoorbeeld door het proberen van alle mogelijke sleutels, om de gebruikte sleutel te achterhalen, maar dat dit een onbruikbaar lange rekentijd vergt. Een dergelijke aanval met brute kracht ("brute force attack") is daarom nauwelijks een bedreiging voor de cryptografische beveiliging.

Recent ontdekte aanvallen maken echter gebruik van kennis van het proces, waardoor het aantal mogelijke sleutels drastisch kan worden gereduceerd. Het herleiden van de gebruikte sleutel K en/of de ingangsdata X uit de uitgangsdata Y wordt daardoor binnen aanvaardbare rekentijden mogelijk.

Het principe van de uitvinding, die beoogt dergelijke aanvallen aanzienlijk moeilijker en tijdrovender te maken, is in Fig. 2 schematisch weergegeven. Evenals in Fig. 1 worden aan een (bekend) proces P ingangsdata X en een (geheime) sleutel K toegevoerd om uitgangsdata Y te genereren.

In tegenstelling tot de situatie van Fig. 1 wordt in de situatie van Fig. 2 de sleutel K vanuit een aanvullend proces P* aan het proces P toegevoerd. Het aanvullende proces P* heeft een aanvullende (secundaire) sleutel K* als ingangsdata om, onder invloed van een hulpsleutel K', de (primaire) sleutel K als uitgangsdata te produceren. De sleutel K wordt dus niet, zoals in de situatie van Fig. 1, vanuit een externe bron (bijvoorbeeld een geheugen) aan het proces P toegevoerd, maar wordt door het proces P* voortgebracht uit de aanvullende (secundaire) sleutel K*:

$$K = P^*_{K'}(K)$$

Het is dus de secundaire sleutel K* in plaats van de primaire sleutel K die vooraf is bepaald en die bijvoorbeeld in een sleutelgeheugen (niet getoond) wordt opgeslagen. Overeenkomstig de uitvinding is de primaire sleutel K die aan het proces P wordt toegevoerd niet vooraf bepaald.

De hulpsleutel K' kan een vast opgeslagen, vooraf bepaalde sleutel zijn. Het is ook mogelijk een aanvullend proces P* toe te passen waarin geen hulpsleutel K' wordt gebruikt.

De combinatie van de processen P en P* vormt een nieuw proces, dat schematisch is aangeduid als Q. Aan het proces Q, dat vanwege het

1011800

uitgangsdata Y opleveren. Het zal duidelijk zijn dat de cryptografische veiligheid hierdoor verder wordt vergroot.

In Fig. 4 is schematisch de wijze weergegeven waarop deelstappen van de processen P en P* afwisselend kunnen worden uitgevoerd ("interleaving") teneinde de bescherming tegen aanvallen verder te vergroten. De deelstappen kunnen zogenaamde "rondes" omvatten, zoals bijvoorbeeld bij DES het geval is. Bij voorkeur omvatten de deelstappen echter slechts een of enkele instructies van een programma, waarmee de processen worden uitgevoerd.

In een eerste stap 101 wordt een eerste deelstap P_1 van het proces P uitgevoerd. Vervolgens wordt in een tweede stap 102 de eerste deelstap P_1^* van het aanvullende proces P* uitgevoerd. Evenzo wordt in een derde stap 103 de tweede deelstap P_2 van het proces P uitgevoerd enz. Dit gaat door totdat in stap 110 de laatste deelstap P_n^* van het aanvullende proces P* is uitgevoerd, waarbij omwille van het voorbeeld ervan is uitgegaan dat de processen P en P* evenveel deelstappen omvatten. Indien dat niet het geval is, wordt in stap 110 de laatste overeenkomstige deelstap uitgevoerd, en worden in verdere stappen de resterende deelstappen uitgevoerd.

Door het afwisselen van de deelstappen van het op zich bekende proces P en het (mogelijk eveneens op zich bekende) proces P* kan een reeks van deelstappen worden verkregen, die niet overeenkomt met die van een bekend proces. De aard van het proces is hierdoor moeilijker te herkennen.

Het in Fig. 5 schematisch en slechts bij wijze van voorbeeld weergegeven cryptografische proces P volgens de stand van de techniek omvat een aantal trappen S_i (d.w.z. S_1, S_2, \dots, S_n). In elke trap S_i worden (rechter) data RD_i toegevoerd aan een cryptografische bewerking F_i . Deze cryptografische bewerking kan zelf een aantal deelstappen omvatten, zoals een expansie, een combinatie met een sleutel, een substitutie en een permutatie, die echter omwille van de eenvoud van de tekening niet afzonderlijk zijn aangegeven. De cryptografische bewerking F_i levert bewerkte data FD_i :

$$FD_i = F_i(RD_i).$$

In een combinatiebewerking CC_i (CC_1, CC_2, \dots , de index i geeft steeds de betreffende trap S aan) worden de bewerkte data FD_i met linker data LD_i gecombineerd tot gemodificeerde (linker) data SD_i , die evenals de oorspronkelijke rechter data RD worden doorgegeven aan de volgende

rechter data RD_n' met een hulpwaarde A_n combineren. Wegens $A_1 \otimes A_1 = 0$ worden op deze wijze de maskeringen door de hulpwaarden A_1 verwijderd. Hierdoor is het mogelijk de werkwijze zodanig uit te voeren, dat ondanks het gebruik van de hulpwaarden A_1 de einddata Y gelijk zijn aan die welke met de conventionele werkwijze volgens Fig. 5 zouden zijn verkregen.

Teneinde de invloed van de hulpwaarden A_1 op de resultaten FD_1 van de bewerkingen F_1 uit te sluiten, is bij voorkeur in elke trap S_1 een aanvullende combinatiebewerking AC_1 aanwezig die de rechter data RD_1 combineert met een (primaire) hulpwaarde A_1 voordat deze data aan de cryptografische bewerking F_1 worden toegevoerd. Het resultaat van elke aanvullende combinatiebewerking AC_1 is niet-gemaskeerde rechter data RD_1 , zodat de cryptografische bewerking F_1 op dezelfde data werkt als in het proces van Fig. 5.

Met voordeel kan een verdere combinatiebewerking BC_1 tussen de cryptografische bewerking F_1 en de combinatiebewerking CC_1 zijn ingevoegd met het doel de bewerkte (rechter) data FD_1 met een verdere (secundaire) hulpwaarde B_1 te combineren. Hierdoor kan een maskering van de bewerkte data FD_1 en een verdere maskering van de (gemodificeerde) linker data SD_1' worden bereikt. Bij voorkeur zijn ook de combinatiebewerkingen AC_1 en BC_1 exclusief-of-bewerkingen.

Overeenkomstig een verder aspect van de uitvinding zijn de hulpwaarden A_1 en B_1 gerelateerd. De secundaire hulpwaarden B_1 zijn bij voorkeur door middel van een exclusief-of-bewerking gevormd uit de primaire hulpwaarde A_{1-1} van de vorige trap en de primaire hulpwaarde A_{1+1} van de volgende trap:

$$B_1 = A_{1-1} \otimes A_{1+1}.$$

Dit heeft tot gevolg, dat elke primaire hulpwaarde A_{1+1} die middels een verdere aanvullende combinatiebewerking BC_1 als bestanddeel van de secundaire hulpwaarde B_1 met de bewerkte rechter data FD_1 is gecombineerd telkens in de volgende trap, d.w.z. in trap S_{1+1} , door een combinatiebewerking AC_1 wordt gecompenseerd voordat de betreffende rechter data RD_{1+1} aan de bewerking F_1 worden onderworpen. De (gemaskeerde) rechter data RD_1' die de (gemaskeerde) linker data LD_{1+1}' van de weer volgende trap S_{1+2} vormen worden daar met de primaire hulpwaarde A_{1+1} gecombineerd en aldus gecompenseerd. De hulpwaarde A_{1+1} werkt door in de gemodificeerde data SD_1' , zodat deze tussen twee trappen gemaskeerd blijven.

1011800

in een willekeurige volgorde bepaald. Indien een gecombineerde bewerking F_1' bijvoorbeeld acht tabellen omvat, worden deze acht tabellen, iedere keer dat deze bewerking F_1' opnieuw wordt uitgevoerd, in een andere volgorde bepaald. Deze volgorde kan worden bepaald aan de hand van de inhoud van een volgorderegister, welke inhoud telkens door een toevalsgetal, afkomstig van een toevalsgenerator, kan worden gevormd. Op basis van de inhoud van het volgorderegister kan verder telkens opnieuw een opzoektabel worden samengesteld. Met de opzoektabel kunnen de tabellen in een geheugen worden weggeschreven en later worden uitgelezen.

Volgens een verder aspect van de uitvinding kunnen in aanvulling hierop of in plaats hiervan de elementen van elke tabel in een willekeurige volgorde worden bepaald en/of opgeslagen. Ook met deze maatregel wordt bereikt dat de bescherming tegen aanvallen wordt verbeterd. Ook in dit geval kan een opzoektabel worden toegepast, aan de hand waarvan de elementen later kunnen worden opgevraagd.

De hiervoor genoemde maatregelen kunnen ook worden toegepast in andere uitvoeringsvormen van de uitvinding, zoals die van Fig. 8, of in geheel andere al dan niet cryptografische processen.

De uitvoeringsvorm van Fig. 8 komt grotendeels overeen met die van Fig. 7. In aanvulling op Fig. 7 is in elke trap S_1 , met uitzondering van de laatste trap S_n , een combinatiebewerking HC_1 opgenomen die de rechter data RD_1 met een tertiaire hulpwaarde W_1 combineert. Bij voorkeur is de tertiaire hulpwaarde W_1 gelijk aan de exclusief-of - combinatie van de hulpwaarden A_0 en A_1 :

$$W = A_0 \oplus A_1,$$

waarbij $A_0 \neq A_1$.

Dit heeft het resultaat dat de bewerking HC_1 steeds de nulde hulpwaarde A_0 toevoegt en de eerste hulpwaarde A_1 compenseert. Hierdoor is het mogelijk dat alle cryptografische bewerkingen F_1 in wezen identiek zijn, hetgeen een veel geringere verwerkings- en/of opslagcapaciteit vereist van een processorsysteem waarmee de werkwijze wordt uitgevoerd. In de uitvoeringsvorm van Fig. 8 zijn de bewerkingen F_1'' zodanige aanpassingen van de oorspronkelijke bewerkingen F_1 , dat deze gecorrigeerd zijn voor de hulpwaarde A_1 en bovendien de tertiaire hulpwaarde $W = A_0 \oplus A_1$ met hun resultaat combineren. Met andere woorden, indien $RD_1 \oplus A_1$ aan F'' wordt toegevoerd, is het resultaat gelijk aan $FD_1' = F_1(RD_1) \oplus W$.

1011800

Hoewel in de figuren 2 en 3 steeds een enkel aanvullend proces P* is getoond, kunnen eventueel meerdere processen P*, P**, P***, ... in serie en/of parallel worden gebruikt om de primaire sleutel K af te leiden.

- 5 Het zal deskundigen duidelijk zijn dat vele wijzigingen en aanvullingen mogelijk zijn zonder buiten het kader van de uitvinding te treden.

10. Werkwijze volgens conclusie 8 of 9, waarin de rechter data (RD_i), in elke trap (S_i) en voorafgaand aan de bewerking (F_i'), met de primaire hulpwaarde (A_i) van die trap (S_i) worden gecombineerd.
11. Werkwijze volgens conclusie 10, waarin de bewerkte rechter data (FD_i), volgend op de bewerking (F_i), met een secundaire hulpwaarde (B_i) van die trap (S_i) worden gecombineerd.
12. Werkwijze volgens conclusie 10 en 11, waarin de secundaire hulpwaarde (B_i) van een trap (S_i) gevormd is uit de combinatie van de primaire hulpwaarde (A_{i-1}) van de voorgaande trap en de primaire hulpwaarde (A_{i+1}) van de volgende trap.
13. Werkwijze volgens een van de conclusies 8-12, waarin alle primaire hulpwaarden (A_i) gelijk zijn.
14. Werkwijze volgens een van de conclusies 9-13, waarin de primaire hulpwaarden (A_i) en/of secundaire hulpwaarden (B_i) telkens vooraf met de respectieve bewerking (F_i) zijn gecombineerd.
15. Werkwijze volgens conclusie 14, waarin een gecombineerde bewerking (F_i') meerdere tabellen bevat, en waarin de tabellen elke keer dat het proces (P) wordt uitgevoerd, in een andere volgorde worden bepaald.
16. Werkwijze volgens conclusie 14 of 15, waarin een gecombineerde bewerking (F_i') meerdere tabellen bevat, en waarin de elementen van de tabellen, elke keer dat het proces (P) wordt uitgevoerd, in een andere volgorde worden bepaald en/of opgeslagen.
17. Werkwijze volgens conclusie 16, waarin de volgorde ten behoeve van het uitlezen van de elementen als opzoektabel wordt opgeslagen.
18. Werkwijze volgens een van de conclusies 8-17, waarin de rechter data (RD_i), na elke trap (S_i), met een tertiaire hulpwaarde (W_i) wordt gecombineerd.
19. Werkwijze volgens conclusie 18, waarin de tertiaire hulpwaarde (W_i) in alle trappen behalve de laatste (S_n) gelijk is aan de combinatie van de primaire hulpwaarde (A_i) van de eerste trap (S_i) en de additionele hulpwaarde (A_0), en in de laatste trap (S_n) gelijk is aan 0.
20. Werkwijze volgens een van de conclusies 8-19, waarin het combineren door middel van een exclusief-of-bewerking wordt uitgevoerd.
21. Werkwijze volgens een van de voorgaande conclusies, waarin de data (X) identificatiedata van een betaalmiddel (1) omvatten en de

1/7

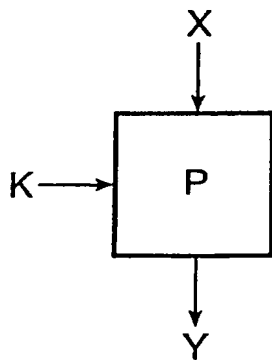


FIG. 1

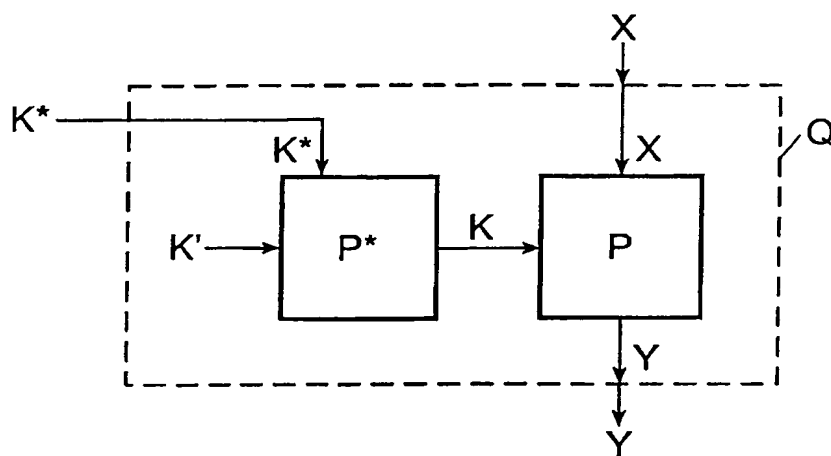


FIG. 2

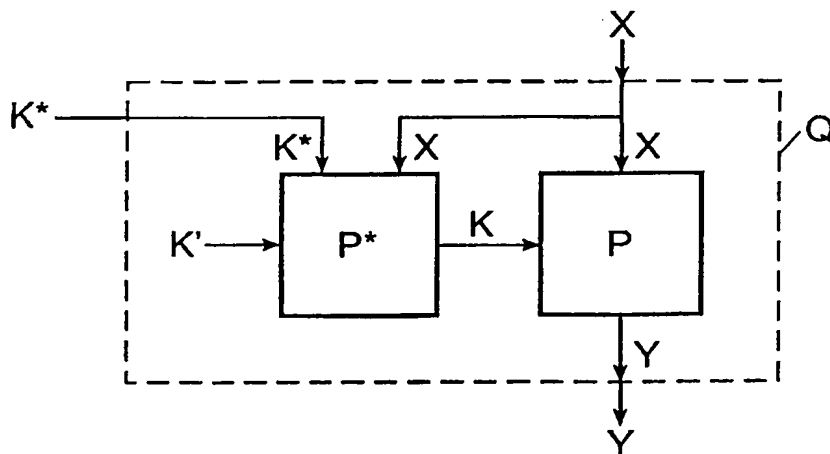


FIG. 3

1011800

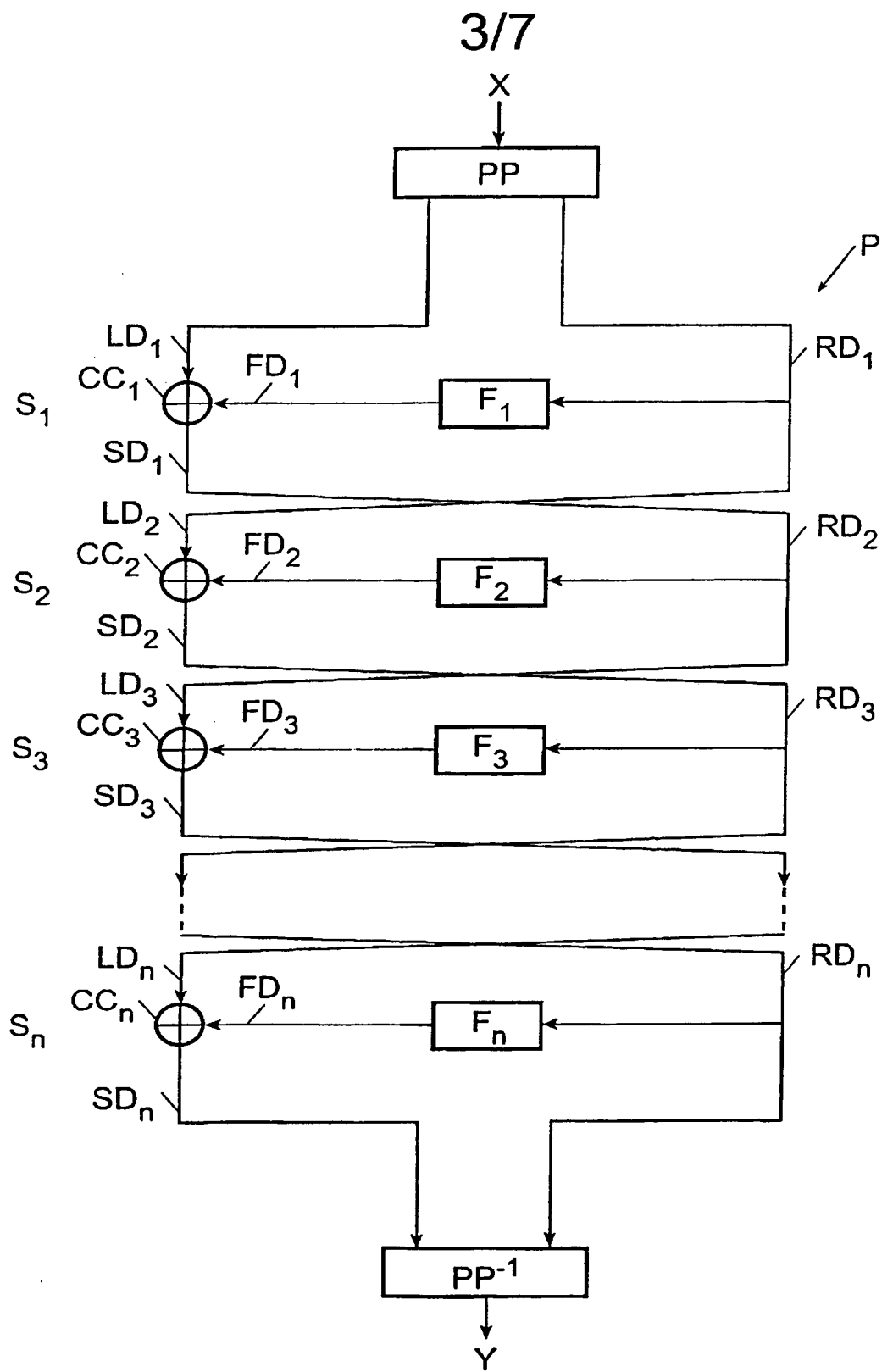


FIG. 5

101 1800

5/7

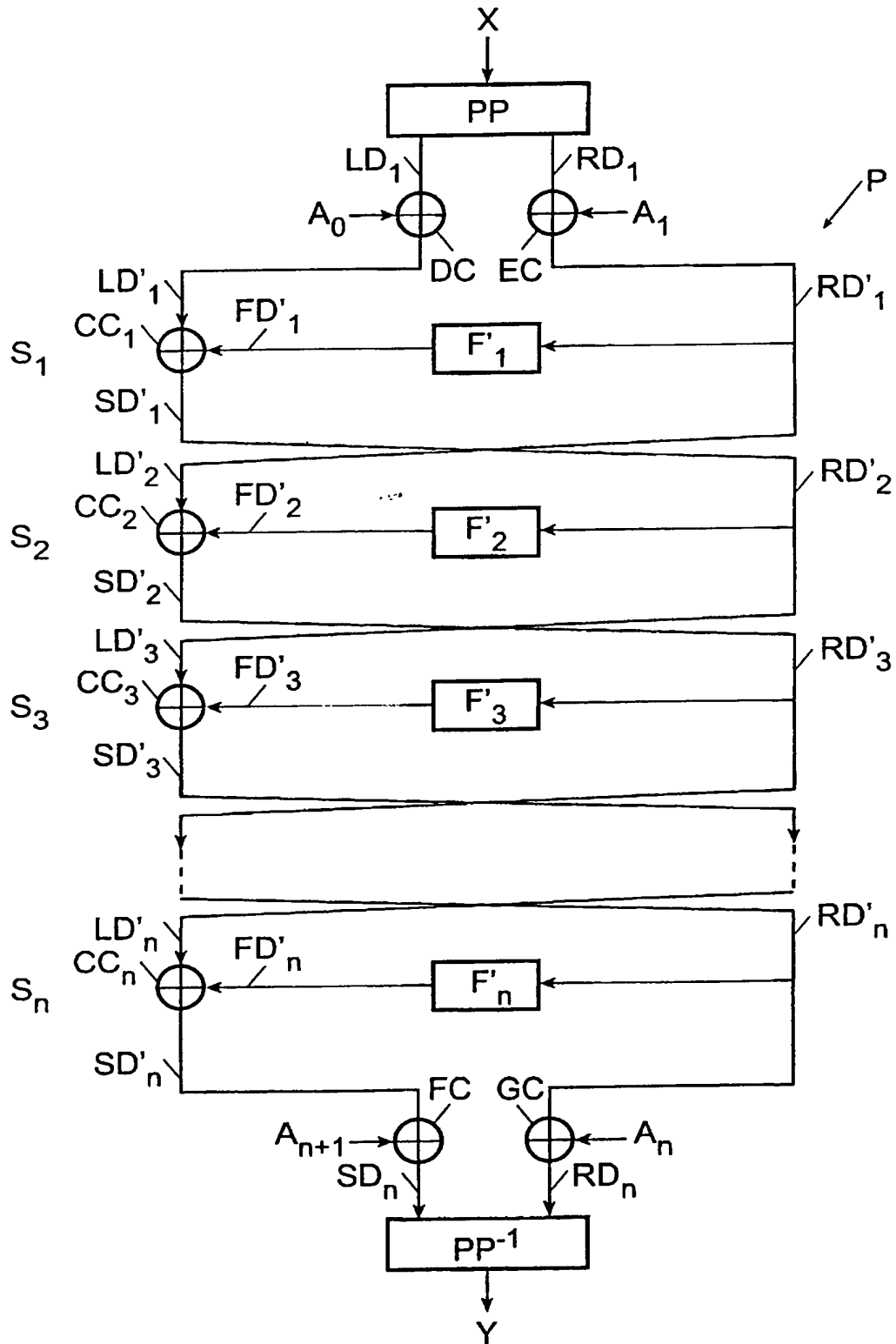


FIG. 7

101 1800

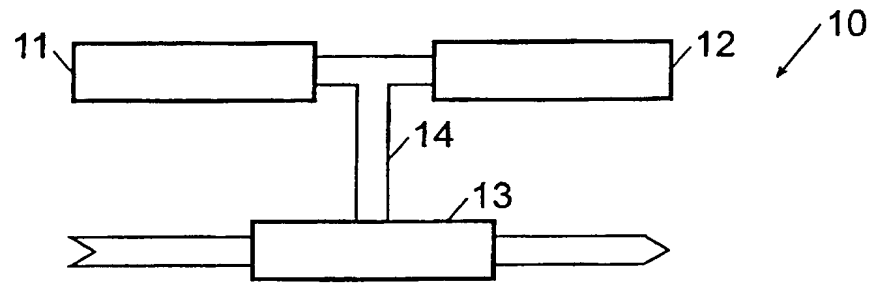


FIG. 9

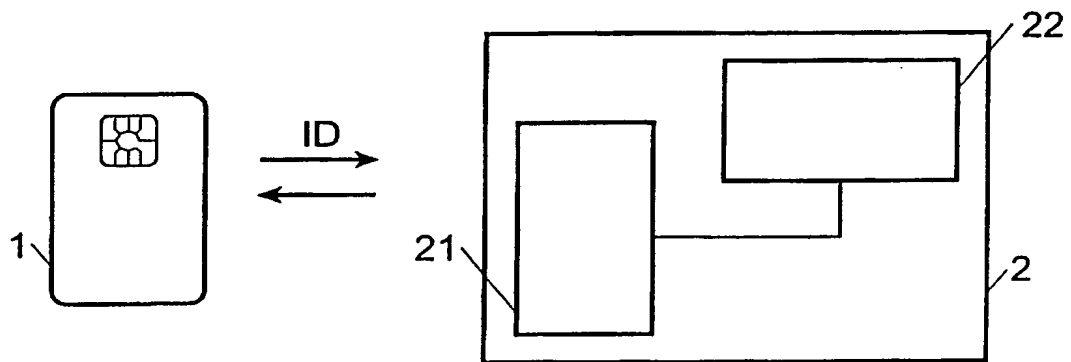


FIG. 10

**VERSLAG VAN HET NIEUWHEIDSONDERZOEK VAN
INTERNATIONAAL TYPE**

Nummer van het verzoek om een nieuwheidsonderzoek

NL 1011800

A. CLASSIFICATIE VAN HET ONDERWERP
IPC 6 H04L9/06

Volgens de Internationale Classificatie van octrooen (IPC) of zowel volgens de nationale classificatie als volgens de IPC.

B. ONDERZOCHE GEBIEDEN VAN DE TECHNIEK

Onderzochte minimum documentatie (classificatie gevolgd door classificatiesymbolen)

IPC 6 H04L

Onderzochte andere documentatie dan de minimum documentatie, voor dergelijke documenten, voor zover dergelijke documenten in de onderzochte gebieden zijn opgenomen

Tijdens het internationaal nieuwheidsonderzoek geraadpleegde elektronische gegevensbestanden (naam van de gegevensbestanden en, waar uitvoerbaar, gebruikte trefwoorden)

C. VAN BELANG GEACHTE DOCUMENTEN

Categorie	Geciteerde documenten, eventueel met aanduiding van speciaal van belang zijnde passages	Van belang voor conclusie nr.
X A	US 5 745 577 A (LEECH MARCUS D) 28 April 1998 (1998-04-28) samenvatting kolom 2, regel 55 - kolom 3, regel 46 kolom 5, regel 6 - kolom 6, regel 4 conclusies 1,6,7 figuren 5,6,8,9 ---	1,2,8, 21-23 3-7,9, 10,13, 18,20
A	US 5 724 428 A (RIVEST RONALD L) 3 Maart 1998 (1998-03-03) samenvatting kolom 5, regel 65 - kolom 6, regel 50 figuren 1B,2 --- -/--	1,2,8, 21,22

☒ Verdere documenten worden vermeld in het vervolg van vak C.

☒ Leden van dezelfde octrooifamilie zijn vermeld in een bijlage

* Speciale categorieën van aangehaalde documenten

- *A* document dat de algemene stand van de techniek weergeeft, maar niet beschouwd wordt als zijnde van bijzonder belang
- *E* eerder document, maar gepubliceerd op de datum van indiening of daarna
- *L* document dat het beroep op een recht van voorrang aan twijfel onderhevig maakt of dat aangehaald wordt om de publikatiedatum van een andere aanhaling vast te stellen of om een andere reden zoals aangegeven
- *O* document dat betrekking heeft op een mondelinge uiteenzetting, een gebruik, een tentoonstelling of een ander middel
- *P* document gepubliceerd voor de datum van indiening maar na de ingeroepen datum van voorrang

T later document, gepubliceerd na de datum van indiening of datum van voorrang en niet in strijd met de aanvraag, maar aangehaald ter verduidelijking van het principe of de theorie die aan de uitvinding ten grondslag ligt

X document van bijzonder belang; de uitvinding waarvoor uitsluitende rechten worden aangevraagd kan niet als nieuw worden beschouwd of kan niet worden beschouwd op inventiviteit te berusten

Y document van bijzonder belang; de uitvinding waarvoor uitsluitende rechten worden aangevraagd kan niet worden beschouwd als inventief wanneer het document beschouwd wordt in combinatie met één of meerdere soortgelijke documenten, en deze combinatie voor een deskundige voor de hand ligt

Z document dat deel uitmaakt van dezelfde octrooifamilie

Datum waarop het nieuwheidsonderzoek van internationaal type werd voltooid

3 September 1999

Verzenddatum van het rapport van het nieuwheidsonderzoek van internationaal type

Naam en adres van de instantie

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040. Tx. 31 651 epo nl,
Fax (+31-70) 340-3016

De bevoegde ambtenaar

Gautier, L

1

INTERNATIONAAL TYPE

Informatie over leden van dezelfde octrooifamilie

In het kader van het verzoek om een nieuwheidsonderzoek

NL 1011800

In het rapport genoemd octrooigeschrift		Datum van publicatie	Overeenkomend(e) geschrift(en)	Datum van publicatie
US 5745577	A	28-04-1998	GEEN	
US 5724428	A	03-03-1998	US 5835600 A	10-11-1998